

Information Security Office - Internal Security Incident Tracking Log
Fourth Quarter FYE 06-30-11 (02-25-11 to 05-26-11)

Attachment 1

Incident Number	Type of Incident	Official Notification Date of Incident Sent to ISOF	Originating Division, Branch, or Office	Comments
11-27 (IN)	Unauthorized Disclosure of SSN for a Deceased Member	02/28/11	HBB	<p>Based on the investigative work performed to date (03-03-11), the ISOF infers on the basis of the evidence collected and examined that the disclosure of the Social Security number for a deceased member, in a non-encrypted e-mail message was not disclosed to the e-mail recipients in an unauthorized manner and does not constitute a breach.</p> <p>The Social Security number for the deceased member is currently available from the United States government and is in the public domain per a search of the FamilySearch™ U.S. Social Security Death Index.</p> <p>The United States Social Security Administration (SSA) publishes the Death Master File (DMF) which the SSA must disclose to the public. The information disclosed in the DMF includes the deceased's Social Security number, first, middle, and surname; dates of birth and death; and state, county and ZIP code of the last address on record.</p>
11-29 (IN)	Unauthorized Disclosure of SSN	03/10/11	BNSD	<p>Based on the investigative work performed to date (03-16-11), the ISOF infers on the basis of the evidence collected and examined that the full Social Security Number for a CalPERS member was disclosed in an unauthorized manner on letter that was mailed to a family member. Per the California State Administrative Manual (SAM), Section 5350.4, Incidents Involving Personal Information, a security breach notification letter offering CSIdentity Theft Insurance was mailed to the member.</p>
11-30 (IN)	Board Member Possible E-Mail Spoof	03/14/11	EPSO	<p>Based on the investigation work to performed to date (03/15/2011), the ISOF infers on the basis of evidence collected and examined that a contact of a CalPERS board member received a targeted SPAM e-mail message. The board member's e-mail account was not subject to e-mail spoofing.</p>

Information Security Office - Internal Security Incident Tracking Log
Fourth Quarter FYE 06-30-11 (02-25-11 to 05-26-11)

Attachment 1

Incident Number	Type of Incident	Official Notification Date of Incident Sent to ISOF	Originating Division, Branch, or Office	Comments
11-31 (IN)	Missing BlackBerry 9700 Bold Smartphone	03/17/11	LPBA	Based on the investigative work performed to date (03-22-11), the ISOF infers on the basis of the evidence collected and examined that a Colliers International issued BlackBerry Bold 9000 smartphone device was lost in a vehicle accident that occurred on February 19, 2011 along Interstate 80 in Fairfield, California. The services to the smartphone device were suspended on February 22, 2011. The device was password protected and a command was issued to wipe all data from the device.
11-33 (IN)	Unauthorized Disclosure of SSN	04/20/11	CSED	Based on the investigative work performed to date (05-12-11), the ISOF infers on the basis of the evidence collected and examined that the full Social Security Number for a CalPERS member was disclosed to another member in an unauthorized manner when her Social Security number was included on two health enrollment forms sent by mistake. A Privacy Breach Notification letter is not necessary pursuant to California Civil Code Section 1798.29 because the unauthorized disclosure involved printed sensitive data on paper documents and did not involve the unauthorized disclosure of electronic sensitive data. However, per the California State Administrative Manual (SAM), Section 5350.4, Incidents Involving Personal Information, a security breach notification letter offering CSIdentity Theft Insurance was mailed to the member.
11-34 (IN)	Unauthorized Disclosure of SSN	04/20/11	ISOF	Based on the investigative work performed to date (05-19-11), the ISOF infers on the basis of the evidence collected and examined that the full names and Social Security numbers for 116 persons had their PII disclosed in an unauthorized manner on the CalPERS Insider. The information on the Insider was removed immediately and both the program and all page masters have been reminded to ensure that private or confidential data is not placed on the Insider. Per the California State Administrative Manual (SAM), Section 5350.4, Incidents Involving Personal Information, a security breach notification letter offering CSIdentity Theft Insurance is being prepared for mailing to the members.

Information Security Office - Internal Security Incident Tracking Log
Fourth Quarter FYE 06-30-11 (02-25-11 to 05-26-11)

Attachment 1

Incident Number	Type of Incident	Official Notification Date of Incident Sent to ISOF	Originating Division, Branch, or Office	Comments
11-35 (IN)	Impersonation of CalPERS Member	04/27/11	CSED	<p>Based on the investigative work performed to date (05-24-11), the ISOF infers on the basis of the evidence collected and examined that an individual (#1) contacted CalPERS via telephone, providing requisite information for identity verification. Person #1 made multiple statements to not change any information on the CalPERS account, specifically the beneficiary information.</p> <p>On April 26, 2011, a separate individual physically visited a CalPERS office, and provided 3 forms of photo identification. Person #2 changed the CalPERS account information.</p> <p>The following day, Person #1 called CalPERS questioning why their account was changed. The CalPERS representative explained to Person #1 that they could physically visit a CalPERS office with 3 forms of photo identification to change the account information back. Person #1 became irate and indicated they would contact their attorney instead.</p> <p>The matter has been referred to the Investigations Unit, which have analyzed Driver's Licenses for both the member and for his wife. The address that was on file prior to the change matches that of the member's wife. The new address that has been updated matches that of the member. The Investigations Unit believes that member's wife is behind the attempts to not update the account. No crime has been reported by the member, so the matter has not been referred to law enforcement.</p>
11-36 (IN)	UserID Phishing Scam	04/28/11	ITSB	<p>Based on the investigative work performed to date (05-06-11), the ISOF infers on the basis of the evidence collected and examined that a potential phishing attempt via e-mail to gain CalPERS user IDs and passwords reached the CalPERS network. In addition, there was no release of confidential information to the phisher.</p>

Information Security Office - Internal Security Incident Tracking Log
Fourth Quarter FYE 06-30-11 (02-25-11 to 05-26-11)

Attachment 1

Incident Number	Type of Incident	Official Notification Date of Incident Sent to ISOF	Originating Division, Branch, or Office	Comments
11-38 (IN)	Unauthorized Disclosure of SSN	40669	BNSD	Based on the investigative work performed to date (05-13-11), the ISOF infers on the basis of the evidence collected and examined that the full Social Security Number for a CalPERS member was disclosed to another member in an unauthorized manner when the Social Security number for a CalPERS member was included on forms and records sent by mistake. A Privacy Breach Notification letter is not necessary pursuant to California Civil Code Section 1798.29 because the unauthorized disclosure involved printed sensitive data on paper documents and did not involve the unauthorized disclosure of electronic sensitive data. However, per the California State Administrative Manual (SAM), Section 5350.4, Incidents Involving Personal Information, a security breach notification letter offering CSIdentity Theft Insurance was mailed to the member.
11-39 (IN)	Key Logger ("Torpig" Malware)	40676	CA OIS	Based on the investigative work performed to date (05-23-11), the ISOF infers on the basis of the evidence collected and examined that the CalPERS assigned Lenovo ThinkPad T400 Laptop computer was not infected with the Torpig malware.